



**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

BETSY FEIST,

Plaintiff,

- against -

PAXFIRE, INC.,

Defendant.

OPINION AND ORDER

11-CV-5436 (LGS) (RLE)

RONALD L. ELLIS, United States Magistrate Judge:

I. INTRODUCTION

Defendant Paxfire (“Paxfire”) moves this Court to dismiss count one of Plaintiff Betsy Feist’s (“Feist”) Complaint, or in the alternative, for sanctions because Feist willfully destroyed material evidence. (Doc. No. 175.) In her Complaint, Feist alleges that Paxfire intentionally intercepted her wire or electronic communications in violation of the Wiretap Act, 18 U.S.C. § 2510 *et seq.* (Doc. No. 1 at 19-20.) According to Paxfire, Feist alleges specific instances of interception and redirection by Paxfire of electronic signals transmitted through Feist’s internet service provider (“ISP”). (Doc. No. 175 at 2.) Paxfire claims that Feist cleared her internet history of visited web pages and cookies, which would have allowed Paxfire to refute Feist’s allegations. (*Id.* at 1.) Feist argues that Paxfire does not need her internet history to defend against the allegations because this action is about Paxfire’s policies and practices, and not merely specific instances of interception and redirection. (Doc. No. 182 at 3.)

For the reasons that follow, Paxfire’s motion for sanctions is **GRANTED IN PART** and **DENIED IN PART**.

II. BACKGROUND

In Count One of her Complaint, filed on August 4, 2011, Feist alleges that Paxfire intentionally intercepted and disclosed her internet searches without her consent in violation of the Wiretap Act. (Complaint ¶¶ 41-43, 45, 47.) For the alleged violations, Feist seeks statutory damages

[w]hich are the greater of (a) actual damages suffered plus any profits made by [Paxfire] as a result of the violation and (b) statutory damages of \$100 per day for each violation, with minimum statutory damages of \$10,000.

(*Id.* ¶ 48.) Feist contends that statutory damages will be based on Paxfire’s “ongoing policies, practices, and conduct,” rather than based on specific instances on interception. (Doc. No. 182 at 6.)

Paxfire counters that a claim for statutory damages per violation means that Feist is alleging specific instances of interception and redirection. (Doc. No. 175 at 2.) Although Feist does not explicitly make the allegation in her Complaint, Paxfire understands Feist to allege that it used a proxy server to intercept the search terms that Feist had entered into a search bar, then redirected certain keywords to third-party merchants, instead of transmitting her searches directly to a search engine. (*Id.* at 3-4.) To defend against Feist’s allegations, Paxfire claims it must be allowed to establish that: “(1) Paxfire did not intercept any of Ms. Feist’s communications; and (2) Paxfire did not redirect any of Ms. Feist’s internet searches.” (*Id.* at 2.) Paxfire also argues that it is entitled to limit or contest statutory damages by identifying the number of specific violations that occurred. (*Id.*) It contends that Feist’s cookies and web browsing history are necessary for this purpose. (*Id.*)

Paxfire explains its role in the redirection of an internet user's search history as follows. ISPs contracted with Paxfire to improve customer internet experiences. (*Id.*) When customers performed internet searches, Paxfire would install cookies on the customer's computer to "obtain a head count of users." (*Id.* at 4.) If a customer was redirected to a website, that visit would be stored on the customer's hard drive. (*Id.* at 4-5.) If Paxfire's cookies did not appear on a computer, Paxfire was not involved in the transmission of that user's communications and search history. (*Id.*) To disprove Feist's claims, Paxfire argues that it would have searched her hard drive to show that there were no cookies on her computer, and therefore no transmission of her internet searches. (*Id.* at 5.) On February 23, 2012, Paxfire asked Feist to produce all devices used to access the internet from January 1, 2007, to the present. Paxfire also asked for her hard drive. (*Id.*, Ex. 2 at 8.) Feist initially objected to production, arguing that the requested information was not relevant. (*Id.*, Ex. 4 at 12.)

Feist's computer crashed in March 2012. (Declaration of Paul McVoy ("McVoy Decl.") at 2; Feist Aug. 17 Deposition ("Dep.") at 368:15.) Paul McVoy, Director of Litigation Support at her counsel's firm, retained a forensic analyst to image Feist's hard drive. (McVoy Decl. at 2.) The analyst was unsuccessful. (*Id.*) On March 20, 2012, a computer engineer attempted to diagnose and repair Feist's computer. (*Id.*) Her files were recovered, and no data was reported lost. (*Id.*) Despite the recovery, Feist's hard drive was still failing. On March 22, 2012, another support engineer replaced her failing hard drive, and transferred data to a new hard drive. He also put a back-up system in place for the new hard drive. (*Id.*) Feist brought the damaged hard drive to her counsel's office on April 4, 2012. On April 12, 2012, UHY Advisors FLVS, Inc. ("UHY") picked up the hard drive from counsel in an attempt to image it. UHY, however, was unable to

access any information on the damaged hard drive. (*Id.* at 3.) On May 9, 2012, a UHY subcontractor was able to recover some data. The drive was sent back to counsel in September 2012, with the recovered information. UHY also provided spreadsheets containing a directory of recovered files and an internet history report with recovered browsing history for each browser used by Feist. (*Id.*) According to McVoy, these documents were provided to Paxfire in May 2012. (*Id.*)

Feist later produced two hard drives on October 3, 2012, to Michael Wudke (“Wudke”), a forensic computer expert retained by RCN Corporation (“RCN”), Paxfire’s former co-Defendant.¹ Wudke was retained to provide an expert opinion on the availability of data on Feist’s personal computer regarding her internet searches and browsing habits. (Doc. No. 175 at 5.) Drive one contained data recovered from Feist’s original hard drive, and drive two was the “original” drive. (Expert Declaration of Michael Wudke (“Wudke Decl.”) at 5.) McVoy maintains that drive two was a back-up drive maintained in the ordinary course of business, which contained documents, and not “machine-created data such as browsing data.” (McVoy Decl. at 4.)

Wudke’s team, TransPerfect, created forensic images of the drives, and searched the images to recover internet history from browsers. According to Wudke, the search identified over 30,000 recovered records, many of which had been last accessed around March 2012. (*Id.* at 7.) TransPerfect found no records of internet history items, or Feist’s search habits with dates prior to March 2012. (*Id.*) TransPerfect also searched for “cleaning” or “wiping” software on both drive images. (*Id.*) Files indicating the installation of a cleaner program were found on drive two. According to Wudke, such programs are used to “delete caches and files related to internet

¹ RCN was terminated on February 6, 2013, upon stipulation of the Parties.

searching and browsing.” (*Id.*) Unlike McVoy’s conclusion that drive two did not contain browsing data, Wudke concluded that the presence of the cleaner program “may explain the absence of internet history records prior to 2012.” (*Id.*) TransPerfect, however, had been unable to determine when the cleaner program was last used, or how frequently it was used because the standard Windows Operating System files were not present on either of the drives. (*Id.* at 8.)

Feist was deposed for a second time on August 17, 2012. During her deposition, she was asked if she had run the cleaner program after filing the Complaint. (Feist Aug. 17 Dep. at 370:16-17.) Feist admitted to running the program after the commencement of this action, but maintained that she did not do so with the intention of destroying evidence. (*Id.* at 370:18-25.) Instead, she ran the program as part of her “computer maintenance.” (*Id.*) She stated that it would have been “too late” to take steps to preserve her internet history, had she been aware that it was relevant to this action. (*Id.* at 368:3-7.) She explained that she had regularly cleaned out her browsing history before July 2011, and there would not have been much information to preserve. (*Id.* at 368:10-13.) She also stated that because her computer crashed, “everything was wiped out at one point.” (*Id.* at 368:15-17.) Feist conceded that she was aware that running the cleaning program would delete her browsing history. (*Id.* at 371:6-11.) She argued that she did not purposefully delete anything, but stated that she also did not “take steps to prevent the deletion of anything.” (*Id.* at 372:10-12.)

III. DISCUSSION

A. Applicable Law

Under Rule 37(e), a party must take reasonable steps to preserve electronically stored information in anticipation or conduct of litigation. “The obligation to preserve evidence arises

when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Treppel v. Biovail Corp.*, 239 F.R.D. 111, 117 (S.D.N.Y. 2008) (citing *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001)). If that information cannot be restored or replaced through additional discovery and the opposing party was prejudiced from the loss, courts have discretion to remedy the loss by measures “no greater than necessary to cure the prejudice.” FED. R. CIV. P. 37(e)(1). If the offending party intentionally acted to deprive its opponent of the information, courts may: (1) presume the lost information was unfavorable to the offending party; or (2) dismiss the action or enter a default judgment. FED. R. CIV. P. 37(e)(2).

Spoliation of evidence occurs when a party destroys or significantly alters evidence, or fails to properly preserve it for another’s use as evidence in reasonably foreseeable litigation. *Alaimo v. Trans World Airlines, Inc.*, No. 00-CV-3906 (GBD), 2005 WL 267558, at *3 (S.D.N.Y. Feb. 3, 2005) (citing *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999)). “For an adverse inference to arise from the destruction of evidence, the party having control over the evidence must have had an obligation to preserve it at the time it was destroyed.” *Kronisch v. U.S.*, 150 F.3d 112, 126 (2d Cir. 1998). Whether to sanction a party for spoliation of discoverable evidence is within the court’s discretion. *W.R. Grace & Co.-Conn. v. Zotos Intern., Inc.*, No. 98-CV-8385 (F), 2000 WL 1843258, at *10 (W.D.N.Y. Nov. 2, 2000). Factors that the court considers include: (1) whether the party acted willfully, negligently, or in bad faith; and (2) the prejudice suffered by the party seeking the discovery. *Id* (citing *John Bo Hull, Inc. v. Waterbury Petroleum Products, Inc.*, 845 F.2d 1172, 1176 (2d Cir. 1988)). If the court chooses to sanction the offending party, the sanction should: (1) deter parties from spoliation; (2) “place the risk of

erroneous judgment on the party who wrongfully created the risk; and (3) restore the prejudiced party to the same position he would have been in absent” the spoliation. *West*, 167 F.3d at 779 (citing *Kronisch*, 150 F.3d at 126).

B. Sanctions Are Warranted

Paxfire argues that Feist had a duty to preserve the evidence of her internet searches on her computer, and that she knew or reasonably should have known that the evidence would be relevant to this action. (Doc. No. 175 at 8.) Paxfire points out that Feist has published two workbooks for children, one of which was for IBM, on basic computer programming in the early 1990s. (Feist Deposition 15:5-13.) It also points out that she took programming courses in college. (*Id.*) Paxfire maintains that Feist did not merely fail to take reasonable steps to preserve electronically stored information. (Doc. No. 175 at 8.) Instead, according to Paxfire, Feist’s conduct was willful because she installed and manually ran a cleaner program after she filed this action, knowing that it would delete her browsing history. (*Id.* at 12.) Furthermore, Feist ran the cleaner program after counsel advised her of her document preservation obligations in this case. (Feist Affidavit ¶ 5.)

Paxfire also claims that Feist acted in bad faith for two reasons: (1) Feist initially said that she *may have* run the cleaner program after filing the lawsuit, but later conceded that she definitely ran it during her deposition; and (2) Feist and her counsel represented that she was producing her original hard drive, which was false. Paxfire argues that Feist never produced her original hard drive, and did not explain why it had been withheld. (Doc. No. 175 at 12-13.) Paxfire’s expert, Wudke, raised concerns about the chain of custody of the two drives that Feist had produced. (Wudke Decl. at 5.) TransPerfect advised Feist that it was unlikely that drive two was her original drive because of the type of drive. It requested clarification of the origin of the drive. (*Id.*) Feist

later indicated that the drive was a backup drive, and not the original as previously stated. According to Wudke, because the drive was not properly preserved, there was no way to determine whether the data had been altered. (*Id.*)

Paxfire argues that Feist destroyed this evidence by cleaning her home computer after filing this action, and prior to producing a copy of her hard drive during discovery. (*Id.*) For Feist's alleged destruction of evidence, Paxfire seeks dismissal of Count One of her Complaint. In the alternative, Paxfire asks that Feist not be allowed to introduce at trial or in her motion for summary judgment, any evidence that Paxfire intercepted specific electronic communication or redirected specific internet searches. (Doc. No. 175 at 14-15.)

Feist contends that she did not act willfully or in bad faith to destroy the evidence of her browsing history. She argues that she had no reason to preserve her browser history because she was not asked to preserve it. (Doc. No. 182 at 7.) Feist testified that it would have been too late to preserve her internet history had she known it was relevant according to Paxfire, because she routinely used the cleaner program prior to the litigation and after it began. (*Id.*) In any event, Feist argues that Paxfire's requested remedies have "little connection to the alleged spoliation" because instances of Paxfire's interceptions may be proved in the form of other evidence aside from Feist's browsing history and cookies. (*Id.* at 9.) For example, other witnesses, expert testimony, and documents may establish that Paxfire violated the Wiretap Act. (*Id.*) Feist also argues that Paxfire is in a better position to argue that the evidence never existed, because Feist no longer has the opportunity to use her internet history to support her claim. (Doc. No. 182 at 9.) According to Feist, Paxfire "may actually have benefited from the alleged spoliation," and thus sanctions are not warranted. (*Id.* at 10.)

The Court is troubled by Feist's assertion that she did not know her browsing history could be relevant to this litigation. Her allegations under the Wiretap Act involve the interception of her internet searches. She is not a novice at computer functioning, and reasonably should have known that evidence of her internet history, including her cookies, would be relevant to this action. Feist admitted running the cleaner program after commencing this action, knowing that it would delete her browsing history. (Feist Aug. 17 Dep. at 371:14.) It is reasonable that prior to filing this action, Feist had used cleaner software to clean up her computer. The use of virus scanners and hard drive cleaning programs is a common occurrence for computer users. It is not reasonable that Feist continued to use the software once this lawsuit began, and did not know that it could prejudice her adversary. In addition to her browsing history, her computer hard drives were instantly relevant. Prior to her computer crashing, Feist did not take any measures to back up her data. The only backup program she possessed was Dropbox, and she claimed not to have stored any files relevant to this action. (Feist Aug. 17 Dep. at 376:13-378:18.)

Because Feist's computer crashed, and both experts have explained that the information is likely not recoverable, additional discovery will not rectify the failure to preserve this evidence. The Court must therefore find a remedy "no greater than necessary" to cure the prejudice of the loss of information. *See* FED. R. CIV. P. 37(e)(1). Paxfire appears to have suffered prejudice. Feist seeks statutory damages for each interception violation per day. Each violation is \$100, for a maximum recovery of \$10,000. Paxfire was therefore entitled to determine and contest the number of violations that occurred, and presumably would have been able to if Feist had not deleted her cookies. The Court, however, does not conclude that Feist acted intentionally to deprive Paxfire of all of the information. There has been no evidence introduced by Paxfire to

dispute the assertion that Feist routinely cleaned her hard drives prior to the litigation. Paxfire has also not shown that Feist was at fault for her computer crashing. Some loss of information was thus unrelated to the litigation.

It is not possible, however, to determine the amount of information that Feist destroyed between the commencement of the litigation in April 2011, and the crashing of her computer in March 2012. At least a year's worth of alleged statutory violations are now undiscoverable. Because Feist does not plead a specific timeframe for Paxfire's alleged interception and redirection, it is possible that all of the statutory violation claims could have occurred in that time frame. By knowingly deleting her browsing history, Feist destroyed evidence that could have allowed Paxfire to raise defenses to the claim for statutory damages. In weighing the factors set out in *West*, the Court finds that sanctioning Feist's conduct is warranted. *See* 167 F.3d at 779. Parties must preserve their hard drives in a timely and reasonable fashion when litigation involves information stored on their personal computers. To hold otherwise would allow the destruction of electronically stored information on computers to go undeterred. Feist must bear the risk of her erroneous judgment in continuing to run the cleaner program after this action was filed.

Part of Paxfire's argument in seeking sanctions is that it will not be able to prove the absence of its cookies on Feist's computer. Therefore the Court presumes that the absence of any cookies is unfavorable to Feist in that she cannot attribute a specific number of redirections to Paxfire.

The Court declines to dismiss Count One of Feist's Complaint, because such a remedy would be disproportionate to the alleged wrongdoing. Feist seeks actual damages for Paxfire's alleged interception, not merely statutory damages based on specific instances of conduct. If there

is other evidence to prove that Paxfire's conduct violated the Wiretap Act such that actual damages can be awarded, Feist is entitled to use that evidence. For example, Feist argues that Paxfire engages in business policies that violate the statute. (Doc. No. 182 at 2-3.) Because Paxfire cannot access Feist's cookies to determine which redirections are attributable to Paxfire's conduct, the Court precludes Feist from arguing that statutory damages are to be awarded in this case for specific redirections, and specific internet searches. Feist may not proffer any evidence of specific violations in its motion for summary judgment, or at trial. Feist is not precluded from using evidence that prove actual damages as alleged in Count One.

IV. CONCLUSION

For the foregoing reasons, Paxfire's motion is **GRANTED IN PART** and **DENIED IN PART**. This resolves Doc. No. 175.

SO ORDERED this 29th day of August 2016.
New York, New York



The Honorable Ronald L. Ellis
United States Magistrate Judge